UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/825,625	04/15/2004	Wieland Fischer	S0193.0017	7860

38881 7590 02/21/2008
DICKSTEIN SHAPIRO LLP
1177 AVENUE OF THE AMERICAS 6TH AVENUE
NEW YORK, NY 10036-2714

EXAMINER	
OKORONKWO, CHINWENDU C	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
02/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/825,625	FISCHER, WIELAND
	Examiner	Art Unit
	CHINWENDU C. OKORONKWO	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Terminal Disclaimer

1. The terminal disclaimer filed on 12/11/2007 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of any patent granted on pending reference Application Number 10827,913, filed on April 19, 2004, has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Amendment

2. In response to communications filed on 12/11/2007, applicant does not amend any of the claims. The following claims, claims 1-11 are presented for examination.

Response to Remarks/Arguments

3. Applicant's arguments, pages 2-4, with respect to the rejection of <u>claims 1-11</u> have been fully considered but they are not persuasive.

3.1 In response to Applicant argument that the Shamir and Boneh references do not teach or suggest verification following the "combining step" of the claim, the Examiner Examiner respectfully disagrees, again citing column 6 lines 17-52 – "w_1=v_1^d_1 (modj*p) and w_2=v_2^d_2 (modj*q), box 24, followed by w_1=v_1^d_1 (modj*p) and w_2=v_2^d (mod j*q), box 26 (*combining step*) … the main observation is that from w_1 and w_2 it is easy to derive y_1 and y_2 b y further reductions … thus it is easy to compute the final result y by the Chinese remainder Theroem". The Shamir reference is

here plainly reciting verification of the two numbers matching after the combining step of box 26.

3.2 In response to Applicant argument that the Boneh reference does not teach or suggest avoiding fault attacks on systems using RSA computations based on the Chinese Remainder Theorem, the Examiner reminder Applicant that this is a 103(a) obviousness type rejection and that the combined Shamir and Boneh references do indeed disclose the argued limitations, citing column 4 lines 50-67 of Shmair which clearly recites “to protect against fault attacks, Boneh [et al.] recommend that each computation should be carried out twice … without incurring the twofold slowdown made necessary by the previously known protective techniques.” Boneh goes on to elaborate on this disclosure in column 5 lines 6-10 which recites “In a fourth embodiment, erroneous signatures of randomly selected messages are each used to obtain a portion of a **secret exponent**. When a sufficient number of bits are obtained, the remaining bits may be “guessed” to obtain the entire secret exponent.”

Based upon the above reasoning the Examiner maintains the rejection of the claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

> matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shamir (US Patent No. 5,991,415) and further in view of Boneh et al. (US Patent No. 6,965,673).

Regarding claims 1, 7 and 11, Shamir, discloses the method and apparatus for protecting an exponentiation calculation wherein the exponentiation calculation is performed within a cryptographic algorithm for an encryption of a message, a decryption of a message, a signature generation from a message or a signature verification calculation from a message, the method comprising: following the combining step, verifying the result of the exponentiation calculation by means of a verifying algorithm, which differs from the combination algorithm, using the first prime number and/or the second prime number, the verifying algorithm providing a predetermined result if the combining step has been performed correctly (col. 5 lines 1-17 and col. 6 lines 17-52 – "w_1=v_1^d_1 (modj*p) and w_2=v_2^d_2 (modj*q), box 24, followed by w_1=v_1^d_1 (modj*p) and w_2=v_2^d (mod j*q), box 26 (*combining step*) … the main observation is that from w_1 and w_2 it is easy to derive y_1 and y_2 b y further reductions … thus it is easy to compute

the final result y by the Chinese remainder Theroem").

Shamir is silent in disclosing calculating the first auxiliary quantity using the first prime number as the module and using the message and calculating the second auxiliary quantity using the second prime number as the module and using the message and then combining the first auxiliary quantity and the second auxiliary quantity using a combination algorithm to obtain a result of the exponentiation calculation (by means of the Chinese remainder theorem using two prime numbers forming auxiliary modules for calculating auxiliary quantities which may be joined to calculate a modular exponentiation for a module equal to the product of the auxiliary quantities) and then suppressing an output of the result of the exponentiation calculation if the verifying step shows that the verifying algorithm provides a result other than the predetermined result, however Boneh does disclose such limitations in column 5 lines 6-10 which recites "In a fourth embodiment, erroneous signatures of randomly selected messages are each used to obtain a portion of a **secret exponent**. When a sufficient number of bits are obtained, the remaining bits may be "guessed" to obtain the entire secret exponent" and column 7 lines 53-57 – "the present versionof the invention will be decribed as a device for obtaining digital signatures for party i. Let N=pq be a product of two lare

prime numbers ... the tamper proof device 200 uses the processor 202 to compute E=m^si where si is a secret exponentstored in the register 206."

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combining the first auxiliary quantity and the second auxiliary quantity using a combination algorithm to obtain a result of the exponentiation calculation – the modulus, since Boneh states in the abstract that comparing a correct signature and an erroneous signature of the same message permit the modulus to be easily obtained, suppressing or discarding erroneous information prevents a hacker or malicious user from cracking the system and signing documents without prior knowledge of the secret exponents (column 4 lines 58-65 and column 7 lines 53-57 of Boneh).

Regarding claim 2, Shamir, discloses method as claimed in claim 1, wherein in addition to the result of the exponentiation calculation, the verifying algorithm uses as input data contents of a memory location at which the first auxiliary quantity, the second auxiliary quantity, the first prime number or the second prime number are stored (column 6 lines 17-52 – "w_1=v_1^d_1 (modj*p) and w_2=v_2^d_2 (modj*q), box 24, followed by w_1=v_1^d_1 (modj*p) and w_2=v_2^d (mod j*q), box 26 (*combining step*) … the main observation is that from w_1 and w_2 it is easy to derive y_1 and y_2 b y further reductions … thus

it is easy to compute the final result y by the Chinese remainder Theroem").

Regarding claim 3, Boneh, discloses method as claimed in claim 1, wherein the exponentiation calculation is an RSA encryption, an RSA decryption, an RSA signature calculation or an RSA signature verification calculation (col. 4 lines 58-65).

Regarding claim 4, Boneh, does not explicitly disclose the combination algorithm is the Garner algorithm, the algorithm is implicitly disclosed because in the Garner algorithm a "large" modular exponentiation is divided into two "small" modular exponentiations in the latter algorithm, the results of which are then united in accordance with the Chinese remainder theorem. Therefore, although not explicitly disclosed the implicit disclosure is clear due to the disclosure of the Chinese remainder theorem in column 4 lines 58-65 and column 5 lines 6-10 of Boneh which recites "In a fourth embodiment, erroneous signatures of randomly selected messages are each used to obtain a portion of a **secret exponent**. When a sufficient number of bits are obtained, the remaining bits may be "guessed" to obtain the entire secret exponent" and column 7 lines 53-57 – "the present versionof the invention will be decribed as a device for obtaining digital signatures for party i. Let N=pq be a product of two lare prime numbers ... the tamper proof device 200 uses the processor 202 to compute E=m^si where si is a secret exponentstored in the register 206."

Regarding claim 5, Shamir, is silent in disclosing a modular reduction of the result of the exponentiation calculation with the first prime number and/or the second prime number as the module however Boneh does disclose obtaining the modulus by means of a first and second signature (col. 4 lines 58-65 of Boneh).

Regarding claim 6, Shamir, discloses method as claimed in claim 1, wherein the first auxiliary quantity is calculated as follows: sp:=m.sup.dp mod p; wherein the second auxiliary quantity is calculated as follows: sq:=m.sup.dq mod q; wherein the combination algorithm is defined as follows: s=sq+{[(sp-sq).multidot.qinv-]mod p}.multidot.q; and wherein the verification algorithm is defined as follows: s mod p=sp; and/or s mod q=sq; and wherein the predetermined result is an equality condition in the verification algorithm (Figure 2 block [30 and 36] col. 4 lines 50-59 col. 6 lines 35-52 and col. 7 lines 22-29).

Regarding claim 8, Boneh, discloses method as claimed in claim 7, wherein a random number is used for verifying auxiliary exponents (column 5 lines 6-10 which recites “In a fourth embodiment, erroneous signatures of randomly selected messages are each used to obtain a portion of a **secret exponent**. When a sufficient number of bits are obtained, the remaining bits may be “guessed” to obtain the entire secret exponent" and column 7 lines 53-57 – “the present versionof the invention will be decribed as a device for obtaining digital

signatures for party i. Let N=pq be a product of two lare prime numbers ... the tamper proof device 200 uses the processor 202 to compute E=m^si where si is a secret exponentstored in the register 206.").

Regarding claim 9, Boneh, discloses method as claimed in claim 7, wherein a prime number is used as input data for verifying the first prime number and the second prime number (col. 4 lines 58-65).

Regarding claim 10, Boneh, discloses method as claimed in claim 9, wherein the prime number has a number of digits which is smaller than the number of digits of the first prime number and of the second prime number (col. 4 lines 58-65).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./

Examiner, Art Unit 2136

February 22, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136